



# FortiAuthenticator™ Token Based SSL VPN

## Solution Guide



## FortiAuthenticator™ Token Based SSL VPN Solution Guide

October 23, 2013

Revision 1

Copyright© 2013 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard® are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation

<http://help.fortinet.com>

Knowledge Base

<http://kb.fortinet.com>

Forums

<https://support.fortinet.com/forums>

Customer Service & Support

<https://support.fortinet.com>

Training

<http://training.fortinet.com>

FortiGuard Threat Research & Response

<http://www.fortiguard.com>

License Agreement

<http://www.fortinet.com/doc/legal/EULA.pdf>

Document Feedback

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)

# Table of contents

Change Log .....	4
Introduction.....	5
Software Versions.....	5
FortiAuthenticator Token Based SSL VPN Guide .....	6
Introduction .....	6
Topology.....	6
FortiAuthenticator Directory Services Configuration .....	6
FortiAuthenticator Adding Tokens .....	7
FortiAuthenticator Assigning Tokens .....	8
FortiToken Mobile for iOS.....	9
FortiAuthenticator RADIUS Client Configuration.....	10
FortiGate RADIUS Client Configuration .....	11
FortiGate SSL VPN Configuration.....	12
Testing, Logging and Monitoring .....	15
Additional Benefits.....	17

# Change Log

Revision	Date	Change Description
1	2013-10-23	Initial revision

# Introduction

This document provides a configuration guide for setting up token based SSL VPNs using the FortiGate and the FortiAuthenticator. The guide provides a step by step walkthrough on both the FortiAuthenticator and the FortiGate, however, for a detailed understanding on the token algorithms and seed handling further reading is required, as the objective of this guide is to provide a configuration walkthrough.

## Software Versions

The configuration discussed in this document was tested on the following firmware versions:

- FortiAuthenticator 3.0
- FortiOS 5.0 GA Patch Release 4

# FortiAuthenticator Token Based SSL VPN Guide

## Introduction

The purpose of this document is to provide a step by step configuration guide on how to setup token based SSL VPNs, using the FortiGate and the FortiAuthenticator. The intention is to provide a concise configuration walkthrough which will allow for the successful deployment of token based VPNs.

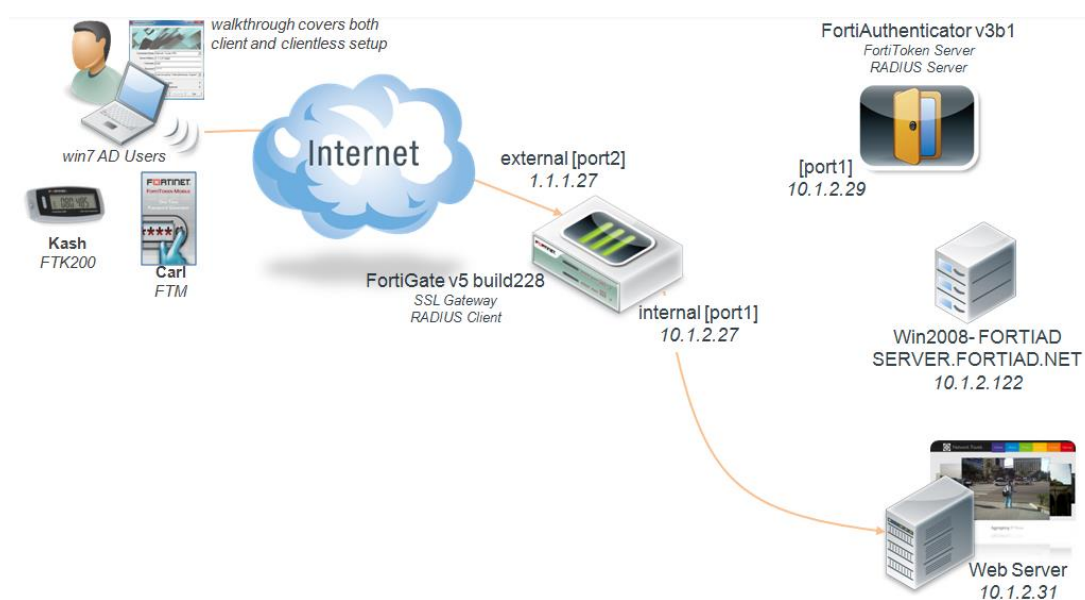
The guide will step through the FortiAuthenticator configuration before moving on the FortiGate, before finally testing the setup. All the topology components are using factory default settings, except for the IP configuration, which is already in place.



**Note:** Before commencing the configuration, please ensure that the date and time are correctly configured and synchronised across all of the topology elements.


If the intention is to use the FortiToken Mobile, please ensure that this is downloaded and installed on the relevant mobile device.

## Topology



## FortiAuthenticator Directory Services Configuration

To commence the configuration on the FortiAuthenticator, the remote user directory services and tokens must be added. Firstly the remote AD/LDAP server must be configured. Within the user interface, under *Authentication>Remote Auth. Servers>LDAP*, click on **Create New**, then complete the AD server settings in a format similar the output below.

Name:	server-2008		
Server name/IP:	10.1.2.122	Port:	389
Base distinguished name:	dc=fortiad,dc=net 		
Bind type:	<input type="radio"/> Simple <input checked="" type="radio"/> Regular		
Username:	cn=admin,dc=fortiad,dc=net	Password:	.....
User object class:	person		
Username attribute:	sAMAccountName		
Group membership attribute:	memberOf		
<b>Secure Connection</b>			
<input type="checkbox"/> Enable			

The username and password required does not necessarily have to be an administrator; the user only requires enough rights to browse the directory for the purposes of pulling users and groups from the directory, into the FortiAuthenticator.

The 'Windows Active Directory Domain Authentication' section does not have to be completed as a requirement for this configuration.

Once the details have been entered, **Click** on the folder icon (next to the base distinguished name field) to ensure that you can browse the directory. If the directory is accessible, then close the browsing window and click on **OK**.

The next step is to import the user (the one intended for SSL remote access) from the directory to the FortiAuthenticator. The user must be in place on the FortiAuthenticator as in the current version (v3.0), unknown user authentication is not supported.

In the user interface go to *User Management>Remote Users* and click on **Import**, then select the relevant pre-defined remote LDAP server and click on import users. From the pop-up window select the relevant user(s) and click on **OK**. The remote user(s), should appear as follows.

				0 of 1 selected	 Search for remote LDAP u:
<input type="checkbox"/>	Username	Remote LDAP server	Admin		
<input type="checkbox"/>	kash	server-2008 (10.1.2.122:389)			

1 remote LDAP user

## FortiAuthenticator Adding Tokens

The next step is to import the tokens into the FortiAuthenticator. Under *User Authentication>User Management>FortiTokens* click on **Create New**. If importing FortiToken200's, then enter the serial number and click on **OK**. At this point the FortiAuthenticator will attempt to access the FortiGuard cloud services and download and install the unique seed associated with the token serial number (the seed is also removed from FortiGuard with this process). The seed download from the FortiGuard cloud is the default import method, it is also possible to order a secure CD with the seed. A successfully imported FortiToken200 should be viewable as follows.

<input type="checkbox"/>	Serial number	Token type	Status	Comment	User	Size	Drift	Timestep
<input type="checkbox"/>	FTK200340H8PL6EF	FortiToken 200	Available			6	0	60

Click on the **Token Serial Number** to edit the Token and from the edit settings click on **'Synchronize'** to synchronise the token. This step is essential to ensure that the token and the FortiAuthenticator are in sync.

If using the FortiToken Mobile (FTM), then the available licenses should be viewable under *Authentication > User Management > FortiTokens*, the FTM tokens are added based on a license file, which is uploaded via *System > Administration > Licensing*. No steps are required with the FortiToken Mobile just yet, other than ensuring that the licenses are visible.

## FortiAuthenticator Assigning Tokens

Once the relevant users and tokens have been imported into the FortiAuthenticator the two elements must be linked together. The process for assigning a FortiToken200 is as follows; within the FortiAuthenticator interface go to *User Management > Remote Users* and click on the **username** the token will be assigned to. From the user edit view check the Token-Based authentication tick box, select FortiToken and apply the relevant token from the FortiToken 200 drop down list (as shown below). If the user settings are correct then click on **OK**.

**System**

- Authentication**
  - User Account Policies
    - Lockouts
    - Passwords
    - Custom User Fields
  - User Management
    - Local Users
    - Remote Users**
    - Remote User Sync Rules
    - User Groups
    - FortiTokens
    - MAC Devices
  - Self-service Portal
  - Remote Auth. Servers
  - RADIUS Service
  - LDAP Service
  - FortiAuthenticator Agent

**Edit Remote LDAP User**

Remote LDAP server: server-2008 (10.1.2.122:389)

Username: kash

Distinguished name: CN=kashif valji,OU=Employees,DC=fortiad,DC=net

☒ Token-based authentication

Deliver token code by: ☒ FortiToken ☐ E-mail ☐ SMS (+44-7768966061)

FortiToken 200: FTK200340H8PL6EF FortiToken Mobile: [Please Select]

[Configure a temporary e-mail/SMS token.](#)

**User Role**

Role: ☐ Administrator ☒ User

**User Information**

**Radius Attributes**

**Certificate Bindings**

**OK** **Cancel**

A successfully assigned FortiToken200 user should be viewable as below.

Username	Remote LDAP server	Admin	Token
cari	server-2008 (10.1.2.122:389)	<input type="checkbox"/>	
kash	server-2008 (10.1.2.122:389)	<input type="checkbox"/>	FortiToken (FTK200340H8PL6EF)

2 remote LDAP users

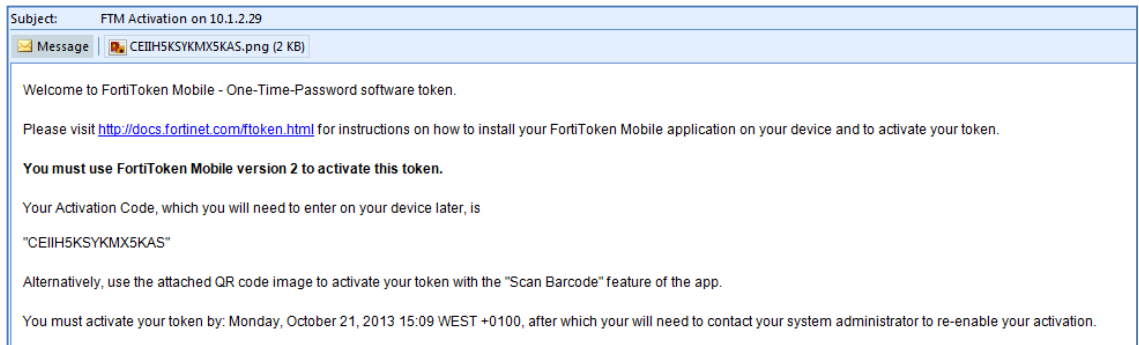
To assign FortiToken Mobile; within the FortiAuthenticator interface go to *User Management > Remote Users* and click on the username the token will be assigned to. From the user edit view check the Token-Based authentication tick box, select FortiToken and apply the relevant token from the FortiToken Mobile drop down list. Ensure that the user has a valid email address configured under the 'User Information' section and that the FortiAuthenticator has the appropriate mail server configuration to email the activation code to the user. It is also possible to send the activation code through SMS, however this requires a valid SMS server such as FortiGuard SMS which requires a valid license. If the user settings are correct then click on **OK**. At this point, the FTM activation code will be sent to the user via e-mail or SMS.

An Active Directory imported user with a FTM assigned should be viewable as follows under *Authentication>User Management>Remote Users*.



FortiAuthenticator				
<div> <div>System</div> <div> <div>Authentication</div> <div> <div>User Account Policies</div> <div> <div>Lockouts</div> <div>Passwords</div> <div>Custom User Fields</div> </div> </div> <div>User Management</div> <div> <div>Local Users</div> <div>Remote Users</div> </div> </div> </div>				
<div> <div>Import</div> <div>Export Users</div> <div>0 of 2 selected</div> <div>Search for remote LDAP u: Search</div> </div>				
Username		Remote LDAP server	Admin	Token
carl		server-2008 (10.1.2.122:389)		FortiToken (FTKM0B3A1847BF12)
kash		server-2008 (10.1.2.122:389)		FortiToken (FTK20034CH8PL6EF)
2 remote LDAP users				

The FTM user should receive an email with the FTM activation code, this should be as follows.



The FortiAuthenticator administrator should be able to view the activation code from the interface under *Logging > Log Access > Logs*, as seen below

FortiAuthenticator

Logged in as admin

Help

Logout

System

Authentication

Fortinet SSO Methods

Monitor

Certificate Management

Logging

Log Access

Logs

Log Config

Log Setting

Syslog Servers

Refresh

Download Raw Log

Log Type Reference

Debug Report

Search for log records

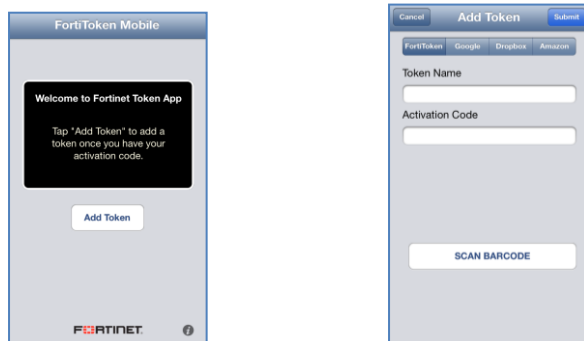
ID	Timestamp	Level	Category	Sub category	Type id	NAS name/IP	Short message
363	Mon Oct 21 14:09:05 2013	information	Event	Admin Configuration	10002		Edited Remote LDAP User: carl @ server-2008 (10.1.2.122:389) (changed fields: FortiToken, alternate...
362	Mon Oct 21 14:09:05 2013	information	Event	System	30908		smtp mail: send to kash@fortinet.com via mail2.fortinet.com 25 ok
361	Mon Oct 21 14:09:03 2013	notice	Event	Admin Configuration	10104		FTM provision: token "FTKM0B3A1847BF12", user "carl", activation code "CEIHH5KSYKMX5KAS"
360	Mon Oct 21 13:33:23 2013	information	Event	Authentication	20002	10.1.2.27	Remote LDAP user authentication with FortiToken successful
359	Mon Oct 21 13:32:57 2013	information	Event	Authentication	20002	10.1.2.27	Remote LDAP user authentication with FortiToken successful
358	Mon Oct 21 13:32:33 2013	information	Event	Authentication	20300	10.1.2.27	Remote LDAP user authentication partially done, expecting FortiToken
357	Mon Oct 21 13:30:06 2013	information	Event	Authentication	20002	10.1.2.27	Remote LDAP user authentication with FortiToken successful
356	Mon Oct 21 13:29:32 2013	information	Event	Authentication	20300	10.1.2.27	Remote LDAP user authentication partially done, expecting FortiToken
355	Mon Oct 21 10:33:22 2013	information	Event	Admin Configuration	10002		Edited Remote LDAP User: kash @ server-2008 (10.1.2.122:389) (changed fields: FortiToken)
354	Mon Oct 21 10:33:22 2013	information	Event	Admin Configuration	10002		Edited FortiToken: FTK20034CH8PL6EF (changed fields: state)
353	Mon Oct 21 02:07:49 2013	notice	Event	System	30905		Changed time to Mon Oct 21 09:27:09 2013
352	Mon Oct 21 02:06:18 2013	information	Event	Authentication	20998		User 'admin' logged in
351	Mon Oct 21 02:06:18 2013	information	Event	Authentication	20998		Local admin authentication with no token successful
350	Mon Oct 21 02:00:05 2013	information	Event	Authentication	20150		Performing a regular check on users with expiring password

## FortiToken Mobile for iOS

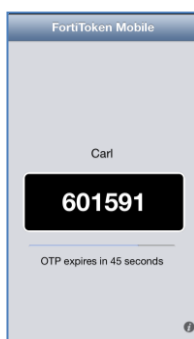
The next few steps address the FTM setup on an iOS compatible device. Once the FortiToken Mobile Application has been downloaded and installed, open the application



Then the activation code prompt will then appear, Tap **Add Token** (if using the application for the first time a PIN will need to be created).



Then enter a token name and the activation code and *Tap **Submit***, if the code is valid, the application should start working immediately and begin prompting the passcode, as shown below.



The passcode prompt displayed by the FTM is used in the same manner as the FortiToken200 passcode prompt.

## FortiAuthenticator RADIUS Client Configuration

The final FortiAuthenticator task is to define the FortiGate as a RADIUS client. Within the interface, go to *Authentication>RADIUS Service>Clients* and click on **Create New**. Then enter the appropriate details (example below) and click on **OK**.

Edit RADIUS Client	
Name:	fgt-10.1.2.27
Client name/IP:	10.1.2.27
Secret:	*****
Description:	
Authentication method:	<input type="radio"/> Enforce two-factor authentication <input checked="" type="radio"/> Apply two-factor authentication if available (authenticate any user) <input type="radio"/> Password-only authentication (exclude users without a password) <input type="radio"/> FortiToken-only authentication (exclude users without a FortiToken)
Authenticate:	<input type="radio"/> All local users <input type="radio"/> Local users from selected groups only (select groups below) <input checked="" type="radio"/> All remote users <input type="radio"/> Remote users from selected groups only (select groups below) <input type="radio"/> All Windows AD users <input type="radio"/> Windows AD users from selected groups only (select groups below)
Remote LDAP server:	server-2008 (10.1.2.122:389) ▼
<input type="checkbox"/> Allow MAC-based authentication	
EAP types:	<input type="checkbox"/> EAP-GTC <input type="checkbox"/> EAP-TLS <input type="checkbox"/> PEAP <input type="checkbox"/> EAP-TTLS

## FortiGate RADIUS Client Configuration

The next set of tasks will be carried out on the FortiGate. Initially the FortiGate needs to be configured as a RADIUS client to the FortiAuthenticator. Within the FortiGate interface, go to *User & Device > Authentication > RADIUS Server* and click on **Create New**. Complete the RADIUS server details, and then test the connection, example below.

**FortiGate VM64**

**Edit RADIUS Server**

Name: FortiAuth-Radius-29

Primary Server Name/IP: 10.1.2.29

Primary Server Secret: [Masked] **Test**

Secondary Server Name/IP: [Empty]

Secondary Server Secret: [Masked] **Test**

Authentication Scheme: ☒ Use Default Authentication Scheme ☐ Specify Authentication Protocol

NAS IP/Called Station ID: [Empty]

Include in every User Group: ☒ Enable

**OK** **Cancel**

Next, a wildcard RADIUS user needs to be created. Go to *User & Device>User>User Definition* and click on **Create New**. Then create a wildcard user as shown below. A wildcard user will allow the FortiGate to send all RADIUS authentication requests to the FortiAuthenticator.

**FortiGate VM64**

**Edit User**

User Name: \*

☐ Disable

☐ Password: [Masked]

☐ Match user on LDAP server: [Please Select]

☒ Match user on RADIUS server: FortiAuth-Radius-29

☐ Match user on TACACS+ server: [Please Select]

Contact Info

☐ Email Address: [Empty]

☐ SMS: ☒ FortiGuard Messaging Service ☐ Custom

Phone Number: [Empty]

☐ Enable Two-factor Authentication

☐ Add this user to groups


**OK** **Cancel**

The next RADIUS configuration step is to create the RADIUS group on the FortiGate which will be host the user(s) for the SSL VPN. Within the FortiGate interface go to *User & Device>User>User Group* and click on **Create New** and create a firewall authentication group that includes the wildcard user and references the FortiAuthenticator, example below.

**Edit User Group**

Name

Type ☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members  

Remote authentication servers

Remote Server	Group Name
FortiAuth-Radius-29	Any

Then go back to the wildcard card user, *User & Device > User > User Definition* and add the wildcard user to the RADIUS group and **OK** the changes, example below.

☒ Add this user to groups

☐ Guest-group

☐ dummy-redirect

☐ fortiad\_net-group

☐ radius

☒ radius-auth

## FortiGate SSL VPN Configuration

The following steps address SSL VPN creation on the FortiGate. Firstly ensure that there is a valid IP pool in place (under *Firewall Objects > Addresses*), if using an IP tunnel based VPN. To begin the SSL configuration, for both IP tunnel based and browser only VPN, go to *VPN > SSL > Config* and ensuring the relevant settings are in place, example below.

**System**

**Router**

**Policy**

**Firewall Objects**

**Security Profiles**

**VPN**

IPsec

Auto Key (IKE)



SSL

Portal

**Config**

Monitor

**SSL-VPN Settings**

IP Pools    
 

---

Server Certificate

Require Client Certificate ☐

Encryption Key Algorithm ☐ High - AES(128/256 bits) and 3DES  
☒ Default - RC4(128 bits) and higher  
☐ Low - RC4(64 bits), DES and higher

Idle Timeout  (seconds)

Login Port

☐ Allow Endpoint Registration (Tunnel Mode Only)

---

**Advanced** (DNS and WINS Servers)

Then under *VPN > SSL > Portal* create the relevant SSL portal interface based on your VPN type (either *IP tunnel* or *browser only*), IP tunnel based VPN is shown in the example below.

**Edit SSL-VPN Portal**

Name:

Portal Message:

Theme:

Page Layout:

☒ Enable Tunnel Mode

☒ Enable Split Tunneling

IP Pools:

Client Options: ☐ Save Password ☐ Auto Connect ☐ Always Up (Keep Alive)

☒ Enable Web Mode

Applications: ☒ HTTP/HTTPS ☐ FTP ☐ RDP ☐ SMB/CIFS  
☐ SSH ☐ TELNET ☐ VNC ☐ PING  
☐ CITRIX ☐ RDP NATIVE ☐ Port Forward

☒ Include Session Info  
☐ Include Connection Tool  
☐ Include FortiClient Download  
☒ Include Bookmarks

Name	Type	Location	Description
<b>Intranet (1)</b>			
Intranet Home	HTTP/HTTPS	10.1.2.31	

Within the FortiGate interface, go to *Policy > Policy* click on **Create New**, then click on VPN setup and create an external interface to internal interface SSL VPN policy, example below.

**Edit Policy**

Policy Type: ☐ Firewall ☒ SSL-VPN

Incoming Interface:

Remote Address:

Local Interface:

Local Protected Subnet:

☐ SSL Client Certificate Restrictive

Cipher Strength:

**Configure SSL-VPN Authentication Rules**

User/Group	Service	Schedule	Security	SSL-VPN Portal	Logging	Action
ANY	ALL	always	-		-	DENY

Comments:  0/1023

From within the policy configuration click on **Create New** under the 'Configure SSL VPN Authentication Rules' section and use the preconfigured RADIUS group and the SSL VPN portal as in the example below, **OK** the changes and then **OK** the main policy.

New SSL VPN Authentication Rule ✕

Group(s)

radius-auth ✕ +

User(s)

Click to add...

Schedule

always ▼

SSL-VPN Portal

tunnel-access ✕

Action

✓ ACCEPT

**Logging Options**

☐ No Log

☒ Log Security Events

☐ Log all Sessions

**Security Profiles**

AntiVirus  
 Web Filter  
 Application Control  
 IPS

default

default

default

default

OK

Cancel

If the completed SSL policy is selected and edited, the configuration should be as follows.

Edit Policy

Policy Type

☐ Firewall ☒ SSL-VPN

Incoming Interface

port2 (external) ▼

Remote Address

all +

Local Interface

port1 (internal) ▼

Local Protected Subnet

webserver [10.1.2.31] +

☐ SSL Client Certificate Restrictive

Cipher Strength

Any ▼

**Configure SSL-VPN Authentication Rules**

+ Create New
 ✎ Edit
 ✕ Delete

User/Group	Service	Schedule	Security	SSL-VPN Portal	Logging	Action
radius-auth	ALL	always	-	tunnel-access	✓	✓ ACCEPT
ANY	ALL	always	-		-	✗ DENY

Comments

Write a comment...

0/1023

OK

Cancel

When configuring an IP tunnel SSL VPN (using the FortiClient), then an additional firewall policy is required (configured *Policy > Policy* and then **Create New**), this is to allow incoming connections from the SSL tunnel interface to the internal network. An example of this is as follows.

New Policy

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	ssl.root (sslvpn tunnel interface) <span style="float: right;">+</span>
Source Address	SSL_RANGE_10_1_2_X <span style="float: right;">+</span>
Outgoing Interface	port1 (internal) <span style="float: right;">+</span>
Destination Address	webserver [10.1.2.31] <span style="float: right;">+</span>
Schedule	always <span style="float: right;">v</span>
Service	ALL <span style="float: right;">+</span>
Action	✓ ACCEPT <span style="float: right;">v</span>
<input type="checkbox"/> Enable NAT	

**Logging Options**

- ☐ No Log
- ☒ Log Security Events
- ☐ Log all Sessions

Once you OK the changes, the completed rule should look as follows in the policy section.

▼ ssl.root (sslvpn tunnel interface) - port1 (internal) (2 - 2)						
2	SSL_RANGE_10_1_2_X	webserver [10.1.2.31]	always	ALL		✓ Accept

This completes the all configuration steps. It is now time to test the VPN.

## Testing, Logging and Monitoring

If the configuration is for a browser only SSL VPN, then open a browser to the SSL VPN gateway. Upon connecting to the gateway, the remote user will land on the standard SSL VPN login page, as below. At the login prompt, enter the directory username and password and then press **Login**.

Please Login

**Name:**

**Password:**

The remote user should then be prompted for a token passcode, as below. Enter the passcode from the FortiToken200 or FortiToken Mobile and click **Login**.

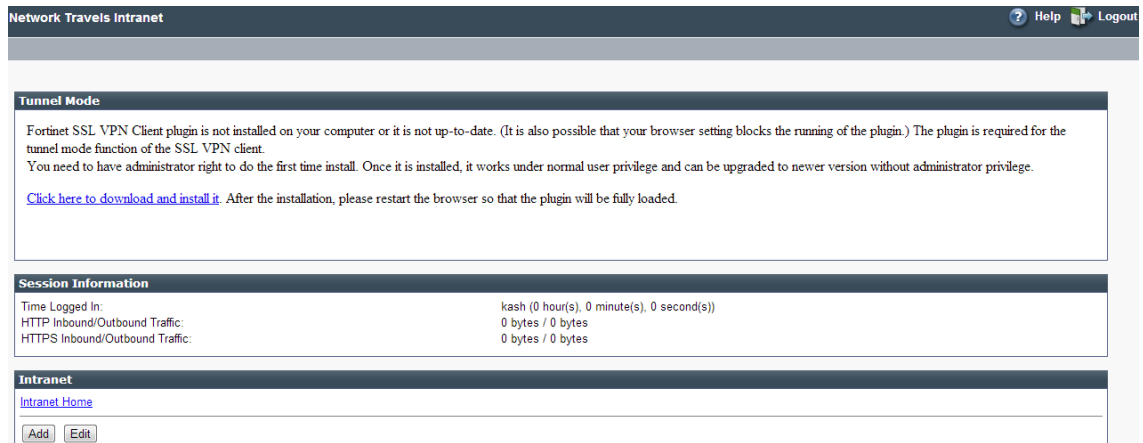
Please Login

**Name:**

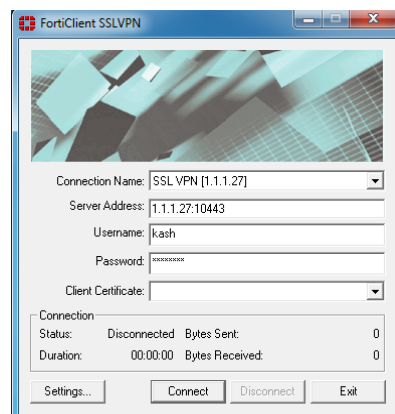
**Password:**

**FortiToken Code:**

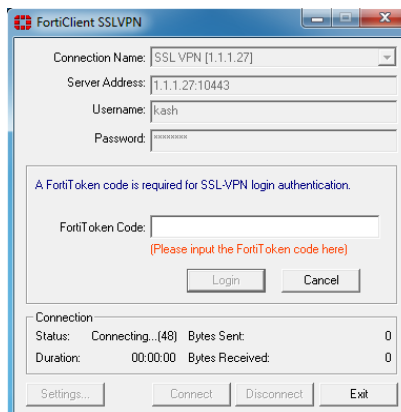
This should then successfully log the user on to the intranet, screenshot below. It is also possible to append the passcode on to the password in the initial login to prevent the passcode prompt.



If using FortiClient SSL, the open the client and complete the connection details and click on **Connect**, example below.



If the username and password is valid, the client will prompt for the token passcode (again this is either from the FortiToken200 or the FortiToken Mobile). If the passcode is correct, the VPN will commence the secure connection.





As with browser based authentication, it is possible to append the token passcode to the initial password to skip the secondary prompt.

Within the FortiAuthenticator user interface, under *Logging > Log Access > Logs* the following entry indicates successful token authentication.

ID	Timestamp	Level	Category	Sub category	Type id	NAS name/IP	Short message
357	Mon Oct 21 13:30:06 2013	information	Event	Authentication	20002	10.1.2.27	Remote LDAP user authentication with FortiToken successful
356	Mon Oct 21 13:29:32 2013	information	Event	Authentication	20300	10.1.2.27	Remote LDAP user authentication partially done, expecting FortiToken
355	Mon Oct 21 10:33:22 2013	information	Event	Admin Configuration	10002		Edited Remote LDAP User: kash @ server-2008 (10.1.2.122:389) (changed fields: FortiToken)
354	Mon Oct 21 10:33:22 2013	information	Event	Admin Configuration	10002		Edited FortiToken: FTK200340H8PL6EF (changed fields: state)
353	Mon Oct 21 02:07:49 2013	notice	Event	System	30905		Changed time to Mon Oct 21 09:27:09 2013
352	Mon Oct 21 02:06:18 2013	information	Event	Authentication	20998		User 'admin' logged in
351	Mon Oct 21 02:06:18 2013	information	Event	Authentication	20998		Local admin authentication with no token successful
350	Mon Oct 21 02:00:05 2013	information	Event	Authentication	20150		Performing a regular check on users with expiring password
349	Mon Oct 21 00:38:34 2013	debug	Event	User Portal	50000		SSO Start login session for user "kash": 0
348	Mon Oct 21 00:38:34 2013	information	Event	User Portal	50000		Remote user 'kash' logged in
347	Mon Oct 21 00:38:34 2013	information	Event	User Portal	50000		Remote LDAP user authentication with no token successful
346	Mon Oct 21 00:38:19 2013	debug	Event	User Portal	50001		SSO Stop login session for user "kash": 0

This completes and confirms the Two-Factor SSL VPN Authentication testing, if the login is unsuccessful the FortiAuthenticator logs should provide indicative information, for detailed debugging please refer to the admin guide.

## Additional Benefits

- FortiAuthenticator can introduce Two-Factor authentication to an existing FortiGate install base with minimal disruption
- With an easy to use interface and rich feature set, customers can increase the security of existing SSL or IPSec VPNs
- FortiAuthenticator supports E-mail and SMS Two-Factor authentication as well as Tokens
- Useful in token vendor migration scenarios
- FortiAuthenticator Two-Factor authentication capabilities can be combined with its Certificate Management capability to provide a comprehensive BYOD solution
- Users and Groups can be auto-imported (based on rules) from the directory server
- Active Directory authenticated users can feed into the FSSO (Fortinet Single Sign-On) framework allowing Identity Based access control across the network

